



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/843,901	04/27/2001	Scott R. Shell	50037.20USU1	9891

27488 7590 04/03/2006

MERCHANT & GOULD (MICROSOFT)
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER

HENNING, MATTHEW T

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 04/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/843,901	Applicant(s) SHELL ET AL.	
	Examiner Matthew T. Henning	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 January 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-28 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 27 April 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

1 This action is in response to the communication filed on 1/13/2006.

2 **DETAILED ACTION**

3 ***Continued Examination Under 37 CFR 1.114***

4 A request for continued examination under 37 CFR 1.114, including the fee set forth in
5 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is
6 eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)
7 has been timely paid, the finality of the previous Office action has been withdrawn pursuant to
8 37 CFR 1.114. Applicant's submission filed on 12/06/2005 has been entered.

9 ***Response to Arguments***

10 Applicant's arguments filed 1/13/2006 have been fully considered but they are not
11 persuasive.

12 In response to applicant's arguments against the references individually, one cannot show
13 nonobviousness by attacking references individually where the rejections are based on
14 combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re*
15 *Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In this particular instance,
16 Rogers disclosed a remote configuration system which has authentication, but does not disclose
17 the details of the authentication. Ho teaches a detailed method for remote authentication.
18 Therefore, the arguments against each reference alone do not apply since the rejection was made
19 in view of the combination of the references.

20 As such, the argument that Rogers did not disclose "identifying a source of the received
21 message from data associated with the received message", the examiner does not find the
22 argument persuasive. Rogers disclosed using encrypted authentication data to provide message

Art Unit: 2131

1 security (Rogers Col. 4 Paragraph 1), but failed to disclose any further details regarding this
2 authentication. The examiner cited page 2 Lines 25-26 of Rogers in order to show the disclosure
3 of encrypted authentication data. Ho on the other hand teaches a messaging system using
4 encrypted authentication data and further identifying a source (the user) of the received message
5 from data in the message (Ho Col. 6 Lines 16-18). Further it can be seen from Fig. 1 of Ho that
6 the message 116 included the identifier information 112. As such the examiner does not find the
7 argument persuasive.

8 The examiner points out that throughout the remarks presented in the communication
9 dated 1/13/2006, the applicants have completely mischaracterized the combination of Rogers and
10 Ho as presented in the final action dated 11/02/2005. Each of the sections of Ho cited by the
11 applicants are not the sections cited by the examiner as meeting various claim limitations. The
12 examiner will particularly point out the incorrect citations and mischaracterizations below.

13 Regarding applicants' argument that Ho did not disclose associating a security role with
14 the received message based on the identified source of the message, the examiner does not find
15 the argument persuasive. The applicants have pointed to Col. 5 Lines 54-59 as the section relied
16 upon by the examiner. On the contrary, the examiner has instead relied upon Col. 6 Lines 33-36
17 to teach such a limitation. In Col. 6 Lines 16-25, Ho teaches that the requester (source of the
18 message) of the information is determined based on identifier information from the received
19 message. Col. 6 Lines 26-36 recite an example where the requestor is a doctor and in Lines 33-
20 36 an appropriate privilege level based on the doctor is determined. Further see Ho Fig. 1 where
21 the message 148 contains the security role 136 that was associated with the user. This meets the

Art Unit: 2131

1 limitation of associating a security role with the received message based on the identified source
2 of the message and therefore the examiner does not find the argument persuasive.

3 Regarding applicants' argument that Ho did not disclose inserting an identifier into the
4 received message to identify the associated security role, the examiner does not find the
5 argument persuasive. Again the applicants have pointed to the incorrect section of Ho by citing
6 Col. 6 Lines 33-36. On the contrary, the examiner has relied upon Col. 6 Lines 37-40 as
7 showing the privilege level being inserted in the message. Fig. 1 Element 148 clearly shows the
8 message containing the access level 136. Therefore, the examiner does not find the argument
9 persuasive.

10 The applicants' argument that Ho is not dealing specifically with configuration messages
11 is further not found persuasive because Ho is not being relied upon to show a teaching of
12 configuration messages, but instead is relied upon for teaching the method of authentication,
13 which Rogers lacks.

14 In response to applicant's argument that there is no suggestion to combine the references,
15 the examiner recognizes that obviousness can only be established by combining or modifying the
16 teachings of the prior art to produce the claimed invention where there is some teaching,
17 suggestion, or motivation to do so found either in the references themselves or in the knowledge
18 generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5
19 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir.
20 1992). In this case, the motivation to combine the authentication system of Ho in the
21 configuration system of Rogers is that Rogers disclosed that authentication could be used, in the
22 system where a single message is provided in order to access and alter configuration information

Art Unit: 2131

1 in a remote device, but did not disclose how to accomplish the authentication. Therefore, the
2 ordinary person skilled in the art would have required an outside teaching of authentication, and
3 Ho teaches an authentication system, in which a single message is authenticated in order to allow
4 access to information in a remote device, which fills the authentication gap of Rogers'
5 disclosure. For this reason, the ordinary person skilled in the art would have been motivated to
6 fill the gap in Rogers using the authentication teachings of Ho. Therefore, the examiner does not
7 find the argument persuasive.

8 In response to applicant's argument that Rogers and Ho are nonanalogous art, it has been
9 held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be
10 reasonably pertinent to the particular problem with which the applicant was concerned, in order
11 to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977
12 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, although Rogers is generally related
13 to the art of configuring a mobile phone using messages, Rogers also suggested the use of
14 authentication in conjunction with the messages (as seen in Col. 4 Lines 15-17). Ho is related to
15 the art of authentication and teaches an authentication method dealing with messages and as such
16 is not nonanalogous art to Rogers. Even more broadly, both pertain to the art of accessing data
17 remotely through messages. Further, the examiner would like to point out that unlike some arts
18 which are very focused on one particular area (i.e. mobile telephones), the art of authentication
19 spans many other areas (i.e. computer networking; access regulation; communications;
20 multimedia; data security; etc.) and when a method of authentication is developed, it is can be
21 used in many different applications. As such, one of ordinary skill in the art at the time of
22 invention would have undoubtedly recognized that the remote authentication method of Ho could

Art Unit: 2131

1 be applied to the remote configuration system of Rogers. As such, the examiner does not find
2 the argument persuasive.

3 Because the applicants' arguments have not been found persuasive, the examiner has
4 maintained the prior art rejection of claims 1-28 below.

5 Claims 1-28 have been examined.

6 All Objections and Rejections not specifically set forth below have been withdrawn.

7 ***Claim Rejections - 35 USC § 103***

8 The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all
9 obviousness rejections set forth in this Office action:

10 *A patent may not be obtained though the invention is not identically disclosed or*
11 *described as set forth in section 102 of this title, if the differences between the subject*
12 *matter sought to be patented and the prior art are such that the subject matter as a*
13 *whole would have been obvious at the time the invention was made to a person having*
14 *ordinary skill in the art to which said subject matter pertains. Patentability shall not be*
15 *negated by the manner in which the invention was made.*

16
17 Claims 1- 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rogers et al.
18 (US Patent Number 6,301,484) hereinafter referred to as Rogers, and further in view of Ho (US
19 Patent Number 6148342).

20 Regarding claim 1, Rogers disclosed a computer-implemented method for maintaining
21 configuration information on a mobile device (See Rogers Abstract), comprising: receiving a
22 message including a request associated with configuration information stored on the mobile
23 device (See Rogers Col. 5 Lines 14-36); identifying the source of the received message from data
24 associated with the received message (See Rogers Col. 4 Lines 13-17); determining at least one
25 configuration setting within the configuration information affected by the received message (See
26 Rogers Col. 6 Lines 45-62); and processing the request associated with the configuration

Art Unit: 2131

1 information (See Rogers Col. 5 Line 34-Col. 7 Line 30) but failed to disclose associating a
2 security role with the received message based on the identified source of the received message;
3 inserting an identifier into the received message to identify the associated security role;
4 comparing the associated security role of the received message with a security privilege
5 associated with the at least one configuration setting on the mobile device; and if the associated
6 security role of the received message is in agreement with the security privilege associated with
7 the at least one configuration setting on the mobile device, processing the request associated with
8 the configuration information. However, Rogers did disclose that authentication data may be
9 used to provide security (See Rogers Col. 4 Lines 15-17), but did not disclose any details about
10 the authentication.

11 Ho teaches a messaging system in which access to data is controlled through
12 authentication (See Ho Abstract, Figs. 1-2 and Col. 5 Line 51 – Col. 7 Line 5). Ho teaches that
13 in order to authenticate access via a message, the source of the message is determined (See Ho
14 Col. 6 Lines 16-18), associates a security role with the received message based on the identified
15 source of the received message (See Ho Col. 6 Lines 34-36), inserts an identifier into the
16 received message to identify the associated security role (See Ho Col. 6 Lines 37-49), comparing
17 the associated security role of the received message with a security privilege associated with the
18 requested access (See Ho Col. 6 Lines 54-60), and if the associated security role of the received
19 message is in agreement with the security privilege associated with the requested access,
20 processing the request (See Ho Col. 6 Line 62-65).

21 It would have been obvious to the ordinary person skilled in the art at the time of
22 invention to employ the teachings of Ho in the configuration system of Rogers by utilizing the

1 authentication protocol of Ho to authorize the configuration changes for each feature code. This
2 would have been obvious because the ordinary person skilled in the art would have been
3 motivated to protect against unauthorized changes.

4 Regarding claim 8, the combination of Rogers and Ho disclosed a computer readable medium
5 having computer executable components for managing security on a mobile device (See Rogers
6 Abstract and further it is well known that processors execute computer instructions in order to
7 function), comprising: a stored setting having an assigned security role that identifies a privilege

8 that an entity attempting to access the stored setting must satisfy in order to access the stored
9 setting (See Rogers Fig. 2 Feature Codes, Ho Fig. 1 Element 157 and Col. 6 Lines 54-61); a

10 router configured to receive a configuration message over a wireless communication link, the

11 router being further configured to identify a source of the configuration message and insert a
12 security role identifier into the received configuration message based on the identified source

13 (See the rejection of claim 1 above and Ho Col. 6 Lines 16-18 and 38-49), the router being

14 further configured to pass the configuration message to other components of the mobile device

15 (See Ho Col. 6 Lines 38-49), the configuration message including an instruction that affects a

16 configuration setting (See Rogers Col. 5 Lines 34-36); and a configuration manager configured

17 to receive the configuration message from the router and to parse the configuration message to

18 identify the configuration setting affected by the configuration message (See Rogers Col. 6 Lines

19 46-62 and Ho Col. 6 Lines 54-61), the configuration manager being further configured to

20 compare the assigned security role of the configuration message to security roles assigned to

21 configuration settings stored on the mobile device (See the rejection of claim 1 above); wherein

22 if the configuration setting identified in the configuration message identifies the stored setting,

1 and wherein if the assigned security role has sufficient privilege to access the stored setting, the
2 configuration manager causes the instruction that affects the configuration setting to be
3 processed (See Ho Col. 6 Lines 54-65 and the rejection of claim 1 above).

4 Regarding claim 13, the combination of Rogers and Ho disclosed a computer-
5 implemented method for maintaining configuration information on a mobile device (See Rogers
6 Abstract; It was also well known that computers have computer executable instructions in order
7 to function), comprising: receiving a configuration message including a header (See Ho Fig. 1
8 Element 112) and an instruction (See Ho Fig. 1 Element 124) associated with a configuration
9 setting stored on the mobile device (See Rogers Col. 5 Lines 14-36); identifying the source of the
10 received message from the header of the received configuration message (See Rogers Col. 4
11 Lines 13-17 and Ho Fig. 1 Element 112); associating a security role with the instruction based on
12 the source of the received message (See Ho Col. 6 Lines 34-36), wherein the associated security
13 role is associated to the instruction by a tag included in the message (See Ho Fig. 1 Element
14 136); comparing the security role of the instruction with a security role associated with the
15 configuration setting stored on the mobile device (See Ho Col. 6 Lines 54-60), and if the security
16 role of the instruction is in agreement with the security role of the configuration setting,
17 processing the instruction (See Ho Col. 6 Line 62-65 and the rejection of claim 1 above).

18 Regarding claim 20, the combination of Rogers and Ho disclosed a computer readable
19 medium within a mobile device, comprising: a data structure associated with a configuration
20 setting being associated with a software component resident on the mobile device, the
21 configuration service provider being responsible for maintaining the configuration setting (See
22 the rejection of claim 1 above and Ho Fig. 1), wherein the data structure comprises: a first field

1 including a security role associated with the configuration setting, the security role of the
2 configuration setting identifying a setting privilege which must be had in order to access the
3 configuration setting (See Ho Fig. 1 Element 132), a second field including a security role
4 identifier, wherein the security role identifier is configured for association with a configuration
5 message (See Ho Fig. 1 Element 136); a third field including a security role associated with the
6 configuration service provider, wherein the security role of the configuration service provider
7 identifies a provider privilege which must be had in order to make use of the configuration
8 service provider, and wherein the third field is configured to determine when the security role
9 identifier matches the security role of the configuration service provider (See Ho Fig. 1 Element
10 157) (See the rejection of claim 1 above).

11 Regarding claims 2 and 14, the combination of Rogers and Ho disclosed that associating
12 the security role with the received message comprises assigning a particular security role based
13 on the source of the message (See the rejection of claim 1 above).

14 Regarding claims 3 and 15, the combination of Rogers and Ho disclosed that the source
15 of the message is identified from authentication and decryption of the received message (See the
16 rejection of claim 1 above and Rogers Col. 4 Lines 13-17 and Ho Col. 6 Lines 16-17).

17 Regarding claims 4 and 16, the combination of Rogers and Ho disclosed that the
18 information within the message includes a shared key that identifies the source of the message
19 (See the rejection of claim 1 above; identifier information).

20 Regarding claims 5 and 17, the combination of Rogers and Ho disclosed that processing
21 the request associated with the configuration information further comprises comparing the
22 security role with another security privilege associated with a configuration service provider, the

1 configuration service provider being responsible for managing the configuration information
2 stored on the mobile device (See the rejection of claim 1 above, Ho Col. 6 Lines 54-60, and
3 Rogers Col. 7 Lines 21-28 wherein each feature code had its own privilege level which needed to
4 be compared).

5 Regarding claims 6 and 18, the combination of Rogers and Ho disclosed that if the
6 security role is not in agreement with the other security privilege the request is not processed
7 (See Ho Col. 6 Lines 54-61).

8 Regarding claims 7 and 19, the combination of Rogers and Ho disclosed that if the
9 security role is in agreement with the security privilege associated with the at least one
10 configuration setting and with the other security privilege associated with the configuration
11 service provider, the configuration service provider processes the request by accessing the
12 configuration information (See Ho Col. 6 Lines 54-63 and Rogers Col. 6 Line 63 – Col. 7 Line
13 6).

14 Regarding claim 9, the combination of Rogers and Ho disclosed a configuration service
15 provider configured to manage at least one configuration setting stored on the mobile device, and
16 wherein the processing of the instruction is performed by the configuration service provider (See
17 Rogers Col. 6 Line 63 – Col. 7 Line 6).

18 Regarding claim 10, the combination of Rogers and Ho disclosed that the configuration
19 service provider has an assigned security role that identifies a privilege that must be associated
20 with an instruction that affects a configuration setting which the configuration service provider
21 maintains (See Ho Col. 6 Lines 16-65).

Art Unit: 2131

1 Regarding claim 11, the combination of Rogers and Ho disclosed that the configuration
2 manager is further configured to determine if the instruction that affects the configuration setting
3 is in agreement with the security role assigned to the configuration service provider that
4 maintains the affected configuration setting, and if so, the configuration manager is further
5 configured to pass the instruction to the configuration service provider to be handled (See Rogers
6 Col. 6 Line 63 – Col. 7 Line 6 and Ho Col. 6 Lines 54-65).

7 Regarding claim 12, the combination of Rogers and Ho disclosed that the configuration
8 service provider determines if the instruction is in agreement with the security role assigned to
9 the stored setting prior to processing the instruction, and if not, terminating the processing of the
10 instruction (See Rogers Col. 6 Line 63 – Col. 7 Line 6 and Ho Col. 6 Lines 54-65).

11 Regarding claim 21, the combination of Rogers and Ho disclosed a configuration
12 message received over a wireless communication link between a source of the configuration
13 message and the mobile device, the configuration message including an instruction to access the
14 configuration setting, the instruction having an associated security role based on the source of the
15 configuration message (See the rejection of claim 1 above).

16 Regarding claim 22, the combination of Rogers and Ho disclosed a configuration
17 manager configured to cause the instruction to be processed if the security role of the instruction
18 is in agreement with the security role of the configuration setting (See Ho Col. 6 Lines 54-65).

19 Regarding claim 23, the combination of Rogers and Ho disclosed a configuration
20 manager configured to cause the instruction to be processed if the security role of the instruction
21 is in agreement with the security role of the configuration service provider (See Ho Col. 6 Lines
22 54-65).

1 37 CFR 1.114. Accordingly, **THIS ACTION IS MADE FINAL** even though it is a first action
2 after the filing of a request for continued examination and the submission under 37 CFR 1.114.
3 See MPEP § 706.07(b). Applicant is reminded of the extension of time policy as set forth in 37
4 CFR 1.136(a). See MPEP § 706.07(h)VIII.

5 A shortened statutory period for reply to this final action is set to expire **THREE**
6 **MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO**
7 **MONTHS** of the mailing date of this final action and the advisory action is not mailed until after
8 the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period
9 will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR
10 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however,
11 will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this
12 final action.

13 Any inquiry concerning this communication or earlier communications from the
14 examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790.
15 The examiner can normally be reached on M-F 8-4.

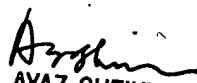
16 If attempts to reach the examiner by telephone are unsuccessful, the examiner's
17 supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the
18 organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

1 Information regarding the status of an application may be obtained from the Patent
2 Application Information Retrieval (PAIR) system. Status information for published applications
3 may be obtained from either Private PAIR or Public PAIR. Status information for unpublished
4 applications is available through Private PAIR only. For more information about the PAIR
5 system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR
6 system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

7
8
9
10 

11 Matthew Henning
12 Assistant Examiner
13 Art Unit 2131
14 3/28/2006
15

16

17 AYAZ SHEIKH
18 SUPERVISORY PATENT EXAMINER
19 TECHNOLOGY CENTER 2100